Permutation Reconstruction

Rebecca Smith

Department of Mathematics
SUNY Brockport, Brockport, NY 14420, USA
rebecca@brockport.edu

Submitted: May 5, 2006; Accepted: Jun 21, 2006; Published: Jun 30, 2006
Mathematics Subject Classifications: 05C05

Abstract

In this paper, we consider the problem of permutation reconstruction. This problem is an analogue of graph reconstruction, a famous question in graph theory. In the case of permutations, the problem can be stated as follows: In all possible ways, delete k entries of the permutation $p = p_1p_2p_3...p_n$ and renumber accordingly, creating $\binom{n}{k}$ substrings. How large must n be in order for us to be able to reconstruct p from this multiset of substrings? That is, how large must n be to guarantee that this multiset is unique to p? Alternatively, one can look at the *sets* of substrings created this way. We show that in the case when $k = 1$, regardless of whether we consider sets or multisets of these substrings, a random permutation needs to be of length at least five to guarantee reconstruction. This in turn yields an interesting result about the symmetries of the poset of permutations. We also give some partial results in the cases when $k = 2$ and $k = 3$, and finally we give a lower bound on the length of a permutation for general k.

1 Introduction

The motivation for permutation reconstruction is the unsolved conjecture of Ulam [6], which when translated into the language of graph theory, concerns the unique reconstruction of a graph G from all its subgraphs formed by deleting a single vertex of G and all of its incident edges.

Definition 1.1 *Let p be a permutation of length n. In all possible ways, delete k entries of p. Then renumber (retaining the order) the obtained $\binom{n}{k}$ strings as permutations so that their entries are now $1, 2, 3, ..., n-k$. We will refer to each of these renumbered strings as $(n-k)$-*minors of p. *We will call the multiset of these permutations the $(n-k)$-*minor multiset of p *and denote it $M_k(p)$. Also, we denote by $C_k(p)$ the underlying $(n-k)$-minor set of $M_k(p)$. Note that $C_k(p)$ can also be thought of in terms of pattern containment since $C_0(p) \cup C_1(p) \cup C_2(p) \cup ... \cup C_n(p)$ is the set of patterns contained in p.*

Example 1.2 *Consider the permutation $p = 142536$. If we remove two entries of p in all possible ways, we get the multiset:*
$\{1425, 1423, 1453, 1253, 4253, 1426, 1456, 1256, 4256, 1436, 1236, 4236, 1536, 4536, 2536\}$
After renumbering and reordering, we have
$M_2(142536) = \{1234^3, 1243, 1324^5, 1342, 1423, 2143, 2314, 3124, 3142\}$ *and*
$C_2(142536) = \{1234, 1243, 1324, 1342, 1423, 2143, 2314, 3124, 3142\}$

Let N_k^M be the smallest number such that the $(n-k)$-minor multiset $M_k(p)$ of a permutation p of length $n \geq N_k^M$ uniquely determines p. That is, each permutation of length $n \geq N_k^M$ gives a unique multiset of $(n-k)$-minors, but there is a pair of permutations p and q, each of length $N_k^M - 1$, where $M_k(p) = M_k(q)$. Let N_k^C be the corresponding number obtained when $M_k(p)$is replaced with $C_k(p)$. Clearly, $N_k^M \leq N_k^C$ for any value of k. In the next sections, we prove that $N_1^M = N_1^C = 5$ and that $N_2^M = 6 < N_2^C$.

2 The Case when $k = 1$

Perhaps surprisingly, we show not only that every permutation of length five or greater can be uniquely reconstructed from its $(n-1)$-minors, but also that it doesn't matter whether we use the set or multiset of $(n-1)$-minors.

Proposition 2.1 *Let p be a permutation of length $n \geq 5$. Then the $(n-1)$-minor set of p, $C_1(p)$, is unique to p. That is, $N_1^C \leq 5$.*

The proof presented here relies on looking at factors of both the original permutation as well as its $(n-1)$-minors. We include the definition of a factor below. Also, we will use the notation $a \star b$ to indicate that there is at least one entry between a and b. This proposition has also been proved independently by Ginsburg [2] and Raykova [4].

Definition 2.2 *A permutation $p = p_1p_2...p_n$ is said to contain a* factor *$q = q_1q_2...q_k$ if p contains q as a contiguous subword.*

Proof: Let p be a permutation of length $n \geq 5$. We will first show that one can determine in which position in p the 1 is, and whether p has a factor of 12, 21 or neither by looking only at $C_1(p)$.

If 1 is in the i^{th} position in p, then consider the position of 1 in the $(n-1)$-minors of p. When the original 1 is not the entry removed, we would have 1 in either the i^{th} or $(i-1)^{st}$ position in any of the resulting $(n-1)$ minors. In the case when the original 1 is the entry removed, the position of 1 in an $(n-1)$-minor is determined by the entry 2 in p.

It is clear where the 1 should be in p if it only shows up in one position in any of the $(n-1)$-minors since it will have to be the first or last entry of p in order for this to have a chance of happening. Note that when 1 only shows up in a single position in any of the $(n-1)$-minors, if 1 is in the first position, p has a factor of 12 and if 1 is in the last position, p has a factor of 21.

If there are only two positions that 1 appears in when considering all of the $(n-1)$-minors in the set, then we have three possibilities. The first is that these positions are the first position and j^{th} position. It can be seen that if there is more than one $(n-1)$-minor with 1 in the first position or if $j > 2$, then 1 must have been in the first position of p and there is not a factor 12 or 21. Otherwise, there is one $(n-1)$-minor with 1 in the first position and the rest have 1 in the second position. This can be seen to force p to be of the form $1 \star 2...$ or $21....$ However, 1 must be in the second position in p since it is clear that removing the second entry from a permutation of the form $1 \star 2...$ results in a different $(n-1)$-minor than removing the fourth entry, but both minors begin with 1. (Clearly p has a factor of 21 in this case since $p = 21....$) The second possibility is that 1 appears in the j^{th} and $(n-1)^{st}$ positions of the minors. The reasoning used to determine where the 1 is in p and whether p has a factor of 12 or 21 from this information parallels that of the argument above. Finally, we have the possibility that 1 appears in position j and $j+1$. (It is not hard to see why these positions must be adjacent given that $1 < j < j+1 < n-1$.) In this case, 1 must be in the $(j+1)^{st}$ position in p since the removal the element in the first position in p would cause the 1 to shift down one position in the resulting $(n-1)$-minor. It is then also clear that 2 must be in position j in p, thus p has a factor of 21.

The final scenario to consider occurs when there are three different positions which the 1 appears in within the set of $(n-1)$-minors. At least two of these positions must be adjacent and if exactly two are, then 1 appears in the further right of the said adjacent positions and there is not a factor of 12 or 21. When all three are adjacent, say $j, j+1, j+2$, then we know that two of the three are $i-1$ and i, so 1 must be in position $j+1$ or $j+2$. In fact, we know that p must have the form $...2 \star 1...$ where 1 is in position $j+2$ or the form $...1 \star 2...$ where 1 is in position $j+1$. If there is more than one $(n-1)$-minor with 1 at a particular position, then that position must be either i or $i+1$. Hence, the only possibility that still presents a problem at this point is when there is a single $(n-1)$-minor at j and a single $(n-1)$-minor at $j+2$. If $j+3 > n$, then the p cannot be of the form $p = ...1 \star 2...$ since this has 2 in the $(j+3)^{rd}$ position, so 1 must be in position $j+2$. Now assume that $j+3 \leq n$. In this case, notice that removing either the $(j+1)^{st}$ entry and then the $(j+3)^{rd}$ entry of $p = ...2 \star 1...$ will result in two distinct $(n-1)$-minors which have the property that 2 appears to the left of 1 and also both have 1 in position $j+1$. There is no way to get two such $(n-1)$-minors from $p = ...1 \star 2...$, so we can determine where 1 is in p in all cases and whether p has a factor of 12 or 21.

To complete the proof, we need to find which minor p' was produced by eliminating the original 1 of p. Then we can simply insert the 1 into the i^{th} position of p' and increase all the other entries by one to get the permutation p. We now consider whether p has a factor of 12, 21, or neither.

1. In the case when p did not contain 12 or 21 as a factor, p' is the $(n-1)$-minor where 1 is not in position i or $i-1$. (Notice that such a minor must exist if neither 12 nor 21 are factors of p.)

2. In the case when p contains the factor 12, we can see that p' is the permutation with shortest factor of the form $123...m$. This is true since eliminating an entry from the factor will decrease the length of it by one. Note that if the original p contains $123...(m+1)$, then eliminating any of the entries $1, 2, ..., m+1$ will result in such a minor, but since the entries are all adjacent, these minors will all be the same.

3. Finally when p contains the factor 21, we can see that p' is the permutation with shortest factor of the form $m(m-1)(m-2)...21$ by the same reasoning as in case 2.

As we have shown how to reconstruct p from $C_1(p)$ in each of the possible cases, the proposition is proved. $\diamond$

Theorem 2.3 $N_1^M = N_1^C = 5$.

Proof: As a result of the previous proposition and since $N_1^M \leq N_1^C$, what remains to be shown is that there is a pair of permutations p and q, each of length four, such that $M_1(p) = M_1(q)$. If we let $p = 2413$ and $q = 3142$, we can check that $M_1(p) = \{132, 213, 231, 312\} = M_1(q)$. $\diamond$

The previous theorem reveals that the poset of permutations S_n ordered by containment has exactly eight symmetries. The previously known symmetries of this poset are those which are generated by reversal, complementation, and inversion. Theorem 2.3 can be used to show that these are the only symmetries of the the poset S_n.

Theorem 2.4 *The poset S_n has exactly the eight symmetries generated by reversal, complementation, and inversion.*

Proof: It is clear that any symmetry must preserve the length of the permutation. As such, we can first focus on the subposet of permutations of lengths 0, 1, 2, 3, and 4 only. One can check that any symmetry of this subposet is generated by reversal, complementation, and inversion. Now let γ be any symmetry of the entire poset. In particular, γ is a symmetry on the subposet of permutations of length less than five. Because of this, on this subposet, $\gamma = \omega$ where ω is generated by the operations of reversal, complementation, and/or inversion. If we can show that $\gamma\omega^{-1}$ must be the identity, then we will have proved that all symmetries of S_n are generated by the operations claimed.

If $\gamma\omega^{-1}$ is applied to S_n, we know that all the permutations of length less than five will be fixed. Also, by induction and Theorem 2.3, we have that any permutation p of length $n \geq 5$ will be fixed since each of these permutations has a unique $(n-1)$-minor set. Hence $\gamma\omega^{-1}$ is indeed the identity permutation. $\diamond$

3 The Case when $k = 2$

When $k = 2$, the question becomes much more complex because there are so many more possibilities. Because of this, simple yet time-consuming computer programs are used to aid the process. One immediate consequence of this was the discovery that $N_2^M \neq N_2^C$. We have been unable to evaluate N_k^C for $k > 1$, but with some computer calculations, we have obtained nontrivial lower bounds for $k = 2$ and $k = 3$.

Proposition 3.1 $N_2^C > 6$.

Proof: We give two permutations $p = 132465$ and $q = 132546$ who have the same $(n-2)$-minor set. In fact, $N_2^C(p) = \{1234, 1243, 1324, 2134, 2143\} = N_2^C(q)$. Hence a permutation must be of length at least seven to guarantee reconstruction from its $(n-1)$-minor set. $\diamond$

It is worth noting that our computer calculations revealed no pair of permutations of length seven having the same $(n-2)$-minor set, so we also know that $N_2^C \neq 8$.

We now consider the question of reconstruction in terms of $(n-2)$-minor multisets. We show that $N_2^M = 6$ implying that the multiplicity of minors does have an impact. This result first appeared in [5].

Proposition 3.2 *Let p be a permutation of length $n \geq 6$. Then $M_2(p)$ is unique to p.*

Proof: Using a computer, we showed that $M_2(p)$ uniquely determines p if the length of p is six or seven. We may now consider the case when the length of p is at least eight. We will use induction on the entries of p. First, take into account the position of 2 relative to the position of 1 in p. In the $\binom{n-2}{2}$ cases when neither the original 1 or 2 of p is eliminated, we get that in the resulting $(n-2)$-minors, the 1 is on the same side of 2 as in p. Since $\displaystyle\binom{n-2}{2} > \frac{\binom{n}{2}}{2}$ when $n > 7$, we can determine which side of 1 the 2 is on in p from the $(n-2)$-minors of p.

Now set aside $\binom{n-2}{2}$ of the $(n-2)$-minors where 1 is on the same side of 2 as it is in p. The remaining $(n-2)$-minors determine where 3 is relative to 1 and 2. Notice that when exactly one of 1 or 2 is eliminated and 3 is not, the 3 acts as a 2 in the resulting $(n-2)$-minors. The final cases occur when two of 1, 2 and 3 are eliminated and 3 acts as the 1 or is not included at all.

If in $0 \leq k \leq 3$ of these $(n-2)$-minors, 1 is to the left of 2, then 3 is to the left of both 1 and 2, if in $n-3 \leq k \leq n$ of these $(n-2)$-minors, 1 is to the left of 2, then 3 must be between 1 and 2, and if in $2n-6 \leq k \leq 2n-3$ (all but at most three) of these $(n-2)$-minors, 1 is to the left of 2, then 3 is to the right of both 1 and 2.

Since $n \geq 8$, all of these cases are distinct and we can thus determine where 1, 2, and 3 are relative to one another. Now suppose we can determine where $1, 2, 3, ..., i$ are relative to one another. Then we will show how to determine where $i + 1$ is relative to

$1, 2, 3, ..., i$. Using another induction argument here, we will first show how to find where $i + 1$ is relative to 1, 2, and 3.

Consider where 1 is relative to $i - 1$ in the $(n - 2)$-minors of p. These can all be found by where $1, 2, 3, ..., i$ are relative to each other except for the following cases:

$\binom{i-1}{2}$ times this is determined by where 1 is relative to $i + 1$,
$i - 2$ times this relative order is determined by where 2 is relative to $i + 1$, and
one time this is determined by where 3 is relative to $i + 1$.

Since we know where 1, 2, and 3 are relative to one another, this determines where $i+1$ is relative to 1, 2, and 3. Now suppose we know where $i+1$ is relative to $1, 2, ..., k-1$. To find where $i + 1$ is relative to k, consider where $k - 2$ is relative to $i - 1$ in the $(n - 2)$-minors of p. Except in the case where these two entries come from k and $i + 1$, we know where $k - 2$ and $i - 1$ should be relative to one another in the $(n - 2)$-minors of p. Simply look at the remaining minors to determine where k is relative to $i + 1$ in p. Because we can determine where all the entries are relative to one another, we can find p from its $(n - 2)$-minors. $\diamond$

Theorem 3.3 $N_2^M = 6$.

Proof: Given the previous proposition, all we need to do is show is that there is a pair of permutations p and q, each of length five, such that $M_2(p) = M_2(q)$. If we let $p = 13524$ and $q = 14253$ we can check that $M_2(p) = \{123^3, 132^4, 213, 231, 312\} = M_2(q)$. $\diamond$

4 The Case when $k = 3$

Once again, in the case of set of $(n - 3)$-minors, we can only report a bound on N_3^C. We give an example to show the following proposition.

Proposition 4.1 $N_3^C > 8$.

Proof: Let $p = 13254768$ and $q = 21354768$. Then we have
$C_3(p) = \{12345, 12354, 12435, 13245, 13254, 21345, 21354, 21435\} = C_3(q)$. $\diamond$

In the case of $(n - 3)$-minor multisets, we can show that $N_3^M \geq 13$ by methods used previously, but because the numbers grow too large for our computer program to handle, we only have that and a lower bound of $N_3^M \leq 7$ due to the following example originally appearing in [5]. The exact answer of $N_3^M = 7$ was determined by Raykova in [4].

Example 4.2 *If we let* $p = 135246$ *and* $q = 142536$ *it can be seen that*
$M_3(p) = \{123^{10}, 132^4, 213^4, 231, 312\} = M_3(q)$. *Hence* $N_3^M > 6$.

5 A Lower Bound on N_k^M

This section focuses on minor multisets although the results apply to minor sets as well. First it is useful to note that if we have two permutations whose minor multisets are the same when removing $k-1$ entries at a time, then the minor multisets that result from removing k entries at a time will also be the same. This fact is stated in the following lemma.

Lemma 5.1 *If $M_{k-1}(p) = M_{k-1}(q)$, then $M_k(p) = M_k(q)$.*

The following proposition is due to Miklós Bóna [1]. This proposition gives us a lower bound on what N_k^M can be for any value of k.

Proposition 5.2 *(Bóna) $N_k^M \geq k+4$.*

Proof: By induction on k.

The result has been shown to be true for $k = 1$ and $k = 2$ in the previous sections. Suppose this proposition is true for $k-1$ and we will prove it is also true for k.

To do this, we will show that there exist permutations P and Q each of length $k+3$ such that $M_k(P) = M_k(Q)$. By the induction hypothesis, there exist permutations p and q, both of length $(k-1)+3$ such that $M_{k-1}(p) = M_{k-1}(q)$. Now consider the permutations $1p$ and $1q$ which are obtained by putting a 1 in front of the appropriate permutation and increasing all the other values of the permutation by one. The 3-minors of $1p$ (and similarly $1q$) can be obtained in one of the two following ways.

First, we consider the 3-minors of $1p$ that are obtained when the 1 of the permutation is removed. Then we are also removing $k-1$ entries from the permutation p. In other words, we are simply obtaining the 3-minors of p. We already know that the 3-minors formed in such a way will be the same as when 1 and k other entries of $1q$ are eliminated to form 3-minors of $1q$.

Thus we only need consider the second case when 1 is not one of the entries removed from $1p$. The 3-minors formed in this way will all begin with 1 and then be followed by 2-minors of p (incremented up by one). By the previous lemma, we know that $M_k(p) = M_k(q)$. Hence these minors will also match up with those of $1q$ formed this way.

Therefore $M_k(1p) = M_k(1q)$, so $N_k^M \geq$ (length of $1p) + 1 = k+4$. $\diamond$

This proof can clearly be applied to $(n-k)$-minor sets as well. However, there is now a better bound for larger k shown by Ginsburg [3] and Raykova [4] of $N_k^C > 2k$. Still the exact growth of N_k^M and N_k^C remain unknown.

Acknowledgments

I wish to thank Miklós Bóna for introducing me to this problem. I also wish to thank Bruce Sagan and Vince Vatter for their helpful suggestions. Finally, I am grateful to the referees for improving the clarity of this paper and for pointing out the application involving the poset of permutations.

References

[1] Miklós Bóna, personal communication.

[2] John Ginsburg, Determining a Permutation from its Set of Reductions, Ars Combinatoria, to appear.

[3] John Ginsburg, personal communication.

[4] M. Raykova, Permutation Reconstruction from Minors, preprint.

[5] Rebecca Smith, "Combinatorial Algorithms Involving Pattern Containing and Avoiding Permutations", Ph.D. thesis, University of Florida, 2005.

[6] S. M. Ulam, A Collection of Mathematical Problems. Wiley, New York, 1960.